

## Year 2000 To Do List

These are some practices that are good to follow to make sure you have complete information about your finances.

- It is always a good idea to save records of your financial activity, including your checking and savings account statements, your investment records, your deposit and ATM withdrawal slips, and your loan payments. For Year 2000 preparation, you may want to save your records for the last few months of 1999 and into the Year 2000.
- Before the New Year holiday, we suggest you take out just as much cash as you normally would for any holiday weekend. You will be able to access your accounts at ATMs as usual during the year-end rollover. All of our ATMs have been tested to be Year 2000 ready, as have the systems that run them. Additionally, we have certified our Year 2000 readiness with the MAC network.
- Be aware of Y2K-related fraud. Someone may try to sell you a "Y2K safe" product, service, or investment. Be skeptical if you are asked to give personal or financial information. Remember, no bank representative will ever call you to ask for your account number, PIN, or password.
- Don't become a target of criminals by storing your cash, stock certificates, or safe deposit valuables in places less secure than your financial institution. Your money is safe in an FDIC-insured bank account today, next month, and next year. Standard homeowner's insurance policies typically might only cover \$200 for cash theft or destruction. The FDIC insures deposits up to \$100,000, and you can secure additional deposit insurance if your deposits are structured appropriately.
- If you use a personal computer for financial transactions and record keeping, be sure to back up your files. Check with the makers of your computer hardware and software to see if they are Y2K-compliant.
- It is always a good idea to look at your credit report periodically to make sure it does not contain inaccurate information about your financial reliability. An error in your credit report could result in a higher interest rate on a loan, a rejection for a job or loan application, or other unnecessary complications.

### Systems We Evaluated for Year 2000 Readiness

We evaluated and tested our hardware and software systems, such as:

- Electronic benefits transfer systems (such as direct deposit and direct payment)
- Automated clearing houses
- Wire transfer systems
- ATM networks
- Credit card merchant and issuing systems
- Check clearing systems
- Trust accounting and reporting systems
- Telecommunications systems
- Voice response systems (such as Touch-Tone Banking)
- Embedded software systems (such as security and alarm systems, elevators, telephones, fax machines and heating and cooling systems)
- Third party vendors of critical computer hardware and software

November 1999

Ready for the  
**Year 2000**

We hope you find this information helpful. If you have additional questions about the Year 2000 issue, please contact us at 1-800-523-2378.

You can also email your questions to  
[year2000@wilmingtontrust.com](mailto:year2000@wilmingtontrust.com).

For more information about the readiness of the financial industry, visit the FDIC web site at

[www.fdic.gov](http://www.fdic.gov).



WILMINGTON  
TRUST

Year 2000 Readiness Disclosure

With the new year just around the corner, we are pleased to report that we have met the June 30, 1999 deadline our banking regulators set for Year 2000 (Y2K) readiness goals and believe we are ready for the date change. All of our critical systems have been addressed and successfully tested for the Year 2000. We are confident that, after December 31, 1999, you will continue to receive the same levels of service that you currently enjoy.

We used an organized, systematic approach to prepare our systems for Y2K. We began by centralizing the management of our efforts through the establishment of a Year 2000 Program Office, which is made up of a team of project leaders representing all areas of our company. Each representative coordinated efforts within his or her area of expertise following the same project approach to ensure continuity and efficiency among the project teams.

## We are pleased to report that we have met our June 30, 1999, Y2K readiness deadline.

This approach yielded excellent results. We have upgraded or replaced all of our critical software and hardware and have checked to ensure that they function properly. We have also tested our applications in a forward-dated environment to perform calculations using actual future dates. Year 2000-ready versions of our critical systems have been running in production for at least six months ahead of the date change.

In addition to this internal testing, we have also tested our systems in conjunction with some of our customers, business partners, and other third parties and found that we are prepared for transactions. We have developed contingency plans to follow in the unforeseen event that our operations are affected by the date change to ensure that we can provide the best service possible.

Our efforts, as well as those of other financial institutions, have been closely monitored by the applicable bank regulatory agencies within the Federal Financial Institutions Examination Council. In addition, bank regulators will continue to monitor financial institutions to ensure a smooth transition into the Year 2000.

While preparing our existing systems for Y2K, we have also made technological investments that include a new wire transfer system, the introduction of On-Line Banking, and an improved infrastructure to support around-the-clock customer access.

## What You Should Know About Y2K Frauds

The FDIC and other government agencies believe that Year 2000 presents an opportunity to cash in on people's fears about the unknown. We want to help you spot the warning signs of a potential fraud scheme so that you won't become a victim. Here are some examples:

- You receive an unsolicited offer to "hold" your money until after January 1, 2000 in a place that is supposedly safer than a federally-insured deposit account. The money would only go into the crook's pocket!
- A con artist posing as a bank employee calls to say that, as part of a Year 2000 fix of the bank's computers, you must confirm (actually reveal) your credit card or bank account number. The crook then uses this information to order new credit cards or checks in your name, and goes on a shopping spree.
- A sales person from a company you've never heard of calls to suggest that you buy into an investment that is free of Year 2000 problems and is guaranteed to net a big profit. It is likely that the only one profiting will be the seller, while you get little or nothing in return.

## Your Best defenses

Here are four things you can do to protect yourself from a potential Year 2000 fraud:

### 1. Remember the classic "red flags" of a financial swindle.

- The deal seems too good to be true or doesn't seem to make sense.
- The offer is from an unfamiliar company, often without a street address or direct telephone number.
- The person or company won't give you written details of the offer.

- You are asked to give cash, a check, or your credit card or bank account number before you receive goods or services.
- The sales person uses high-pressure tactics or is intimidating.

Hang up the phone or walk away from any unsolicited offer.

### 2. Protect your personal financial information.

Never give out your Social Security, bank account, or credit card numbers to an unknown person or company unless you initiated the contact, and never give anyone the Personal Identification Number you use to access an ATM. A con artist can use this information to withdraw money from your bank account or order new credit cards in your name. Always confirm with a reliable source whether you do, indeed, have a problem and, if so, whether there isn't a better solution. For example, if you are approached about a supposed Year 2000 problem with your bank account, check with us independently.

### 3. Check out any offer to buy or invest in a product or service before you commit to anything.

If you are seriously considering an offer, get as much information as you can before you agree to pay money. To find out more about a particular company, the Better Business Bureau is an excellent source of information (including complaints against companies).

### 4. Take the time to spot, and report, a possible fraud.

Always review your account statements and credit card bills to make sure a swindler hasn't withdrawn money or made purchases in your name. Also, if one of your bills or statements doesn't arrive in the mail, that could be a sign someone has changed your billing address for fraudulent purposes. If you think you have been the victim of a scam or just suspect fraud, call the police immediately. Then call us.